Unclassified
SECURITY CLASSIFICATION OF THIS PAGE

1a. REPORT SECURITY CLASSIFICATION
Unclassified

2a. SECURITY CLASSIFICATION AUTHORITY
N/A

2b. DECLASSIFICATION / DOWNGRADING SCHEDULE
N/A

3. DISTRIBUTION / AVAILABILITY OF REPORT
Distribution Statement A: Approved for public release; distribution is unlimited.

4. PERFORMING ORGANIZATION REPORT NUMBER(S)
NDU-ICAF-93- A76

5. MONITORING ORGANIZATION REPORT NUMBER(S)
Same

6a. NAME OF PERFORMING ORGANIZATION
Industrial College of the Armed Forces

6b. OFFICE SYMBOL (If applicable)
ICAF-FAP

7a. NAME OF MONITORING ORGANIZATION
National Defense University

6c. ADDRESS (City, State, and ZIP Code)
Fort Lesley J. McNair
Washington, D.C. 20319-6000

7b. ADDRESS (City, State, and ZIP Code)
Fort Lesley J. McNair
Washington, D.C. 20319-6000

8a. NAME OF FUNDING / SPONSORING ORGANIZATION

8b. OFFICE SYMBOL (If applicable)

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS (City, State, and ZIP Code)

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)
Operational and Technical Sigint -- 2020 Foresight?

12. PERSONAL AUTHOR(S) Dennis S. Henderson

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Research	FROM Aug 92 TO Apr 93	April 1993	55

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

SEE ATTACHED

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL
Judy Clark

22b. TELEPHONE (Include Area Code)
(202) 475-1889

22c. OFFICE SYMBOL
ICAF-FAP

DD FORM 1473, 84 MAR

83 APR edition may be used until exhausted.
All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

ABSTRACT

In many respects the 21st Century's New World Order will not be so "new" or so "orderly". The increasing rich/poor dichotomy, overpopulation, rapid urbanization, environmental degradation and disease and rising nationalism will render the international arena more volatile and unstable. Into this morass U.S. troops will be employed to deter and/or fight insurgency, terrorism, proxy warfare and drug trafficking. To support them in this environment, signals intelligence must bury its classical separations which have divided it into four disciplines during the Cold War and must provide fused, operational and technical intelligence covering the entire electromagnetic spectrum. On-going and currently planned programs are leading to such increased capabilities and interoperability -- ***the key is to not let them become new collection programs, but maintain their emphasis on information processing and dissemination which will provide focused, fused, friendly intelligence -- the "cheaper" force multiplier of the 21st Century.***

1993
Executive Research Project
A76

Operational and Technical Sigint--2020 Foresight?

Colonel
Lewis S. Henderson
U.S. Air Force

Faculty Research Advisor
Dr. Abraham Singer

The Industrial College of the Armed Forces
National Defense University
Fort McNair, Washington, D.C. 20319-6000

1993
Executive Research Project
A76

Operational and Technical Sigint--2020 Foresight?

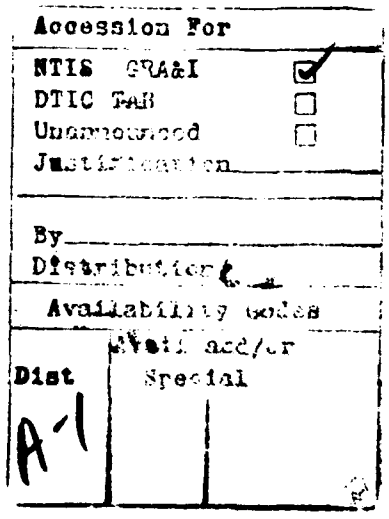
Colonel
Lewis S. Henderson
U.S. Air Force

Faculty Research Advisor
Dr. Abraham Singer

The Industrial College of the Armed Forces
National Defense University
Fort McNair, Washington, D.C. 20319-6000

DISCLAIMER

This research report represents the views of the author and does not necessarily reflect the official opinion of the Industrial College of the Armed Forces, the National Defense University, or the Department of Defense.



ABSTRACT

In many respects the 21st Century's New World Order will not be so "new" or so "orderly". The increasing rich/poor dichotomy, overpopulation, rapid urbanization, environmental degradation and disease and rising nationalism will render the international arena more volatile and unstable. Into this morass U.S. troops will be employed to deter and/or fight insurgency, terrorism, proxy warfare and drug trafficking. To support them in this environment, signals intelligence must bury its classical separations which have divided it into four disciplines during the Cold War and must provide fused, operational and technical intelligence covering the entire electromagnetic spectrum. On-going and currently planned programs are leading to such increased capabilities and interoperability -- ***the key is to not let them become new collection programs, but maintain their emphasis on information processing and dissemination which will provide focused, fused, friendly intelligence -- the "cheaper" force multiplier of the 21st Century.***

The reason the enlightened sovereign and the wise general often win the battle when they move, and their achievements surpass those of ordinary men, is foreknowledge. -- Sun Tzu

The next war will be won by the side that best explo_ s the electromagnetic spectrum. -- Admiral Sergei G. Gorshkov, former commander of the Soviet Navy

A BATTLEFIELD IN THE FUTURE

The cavalry platoon leader views the tactical situation on his reconnaissance/strike vehicle's visual display. Along with his semi-autonomous, robotic outrigger vehicles, he has coalition company. The green blip two kilometers to his right is a vehicle from his cavalry regiment. The blue symbol on his left is another vehicle from one of the allied armies in this combined operation.

On this totally blacked out night, the mission is to reconnoiter and disable any forces found in the sector ahead and report back any reconnaissance over the real time video link to higher headquarters. A constant stream of intelligence information is pouring into each vehicle from headquarters, airborne intelligence platforms and satellite broadcasts. Only seconds to minutes old, the reconnaissance vehicle's vetronics[1] now displays red symbols behind the hills 4000 meters ahead.[2] Automatic cross-correlation of data identifies the enemy as a squadron of tanks and supporting forces on the move, which must be destroyed. The highly automated targeting and weapon system on this two person vehicle has already computed firing parameters

and will soon give a cue on the screen when the target is within the firing envelope.

Already coordination with the J-STARS battlefield surveillance aircraft and the All Source Identification System (ASIS) has automatically re-verified that the target will not become a fratricide statistic. As the target comes within firing range, the intelligence data streams identify and confirm a company's worth of enemy vehicles approaching a vital river junction.

The tactical situation display in the airborne command post shows the same ground targets, as well as displaying the combined forces aircraft streaking to pounce on them in near real time. As the reconnaissance/strike vehicles fire their long range, millimeter wave, terminal homing rounds at the lead vehicles, the fighter pilots launch their long range stand-off attack weapons which will also guide themselves to their individual targets while the aircraft stay out of the range of defensive fire. Meanwhile, an airborne jamming aircraft hooked into the tactical situation net jams the enemy's counter battery radar systems to mask the position of the reconnaissance/strike vehicles.

Near real time weapons damage assessment collected and transmitted back from unmanned air vehicles and other sources simultaneously confirms to all parties that the enemy formation has been destroyed or disabled.

While the above scenario is postulated to occur

sometime around 2020, all of the technologies used above are available today. The biggest challenge is to collect and fuse diverse intelligence data , particularly those dealing with target acquisition and identification, and disseminate that information to the proper individuals in the desired format in near real time.

ORGANIZATION OF PAPER

The central focus of this paper is that Signals Intelligence (SIGINT) must bury its classical separations which have divided it into four disciplines during the Cold War. In the future, intelligence professionals must provide fused, operational and technical intelligence of which SIGINT plays a large part. The intelligence user, particularly operational commanders and "shooters", will not care from what source that his information comes, only that it be readily available to him with coverage of the entire electromagnetic spectrum. Operational commanders and planners will also demand detailed, all source analysis of the capabilities and vulnerabilities of the opponents they face. Thus SIGINT must continue to evolve and expand its horizons into the 21st century to provide a comprehensive SIGINT picture of the order of battle.

We will first briefly look at what SIGINT is currently, to serve as background for what changes should occur for it to remain a viable intelligence input in the 21st Century.

Next I will present a picture of what the operational and

technical SIGINT requirements might be in the year 2020., through postulating some generic, future weapon system characteristics and what those characteristics imply for signals intelligence.

Lastly I will propose some changes that need to be made in the intelligence community to improve and facilitate operational and technical intelligence needs 20-30 years hence.

In God We Trust --
All others we monitor. -- noted in one National Security Agency briefing.

What is SIGINT?

SIGINT is knowledge derived from the interception and processing of communications and non-communications signals. It is composed of four elements. Communications Intelligence (COMINT) is the interception and analysis of communications signals. Foreign Instrumentation Signals (FIS) Intelligence (FISINT) makes up another portion of the SIGINT discipline. FISINT attempts to collect and interpret the data from telemetry and instrumentation systems in order to derive system capabilities and activities. For strategic arms control, the U.S. could count numbers principally through the use of photo satellites, "But the chief means of monitoring the capabilities of these missiles was interception of Soviet missile test telemetry by signals intelligence satellites and ground stations." [3]

"Proforma" or data link signals make up another SIGINT

category which is growing in importance. These are hybrid signals containing the characteristics of both COMINT and Electronic Intelligence (ELINT) signals.

ELINT is defined as, "...intelligence information that is the product of activities in the collection and processing, for subsequent intelligence purposes, of potentially hostile, non-communications electromagnetic radiations which emanate from other than nuclear detonations and radioactive sources."[4]

To hopefully clarify that rather turgid definition permit me to highlight and expand several phrases. ELINT deals with non-communication signals which separates it from COMINT. Basic ELINT targets are all types of radars as well as navigation systems, command and telemetry links and data links as opposed to telephones, radios, teletypes, television, etc.

Non-nuclear and non-radioactive sources mean that the signals are transmitted from some system, a radar, a navigation system, etc. Electromagnetic refers to the type of wave phenomena, in this case we generally think of radio waves used by common radio systems and radars, but the total spectrum of electromagnetic waves covers much more -- extending all the way through visible light, infrared light and ultra-violet (purple) light.

> We do not have to imagine some forms of electromagnetic energy, because we can see it with our eyes in the form of light, we can feel its effect with our skin as heat, and we can hear sounds that have been carried over the air by electromagnetic energy. ... In battle, electromagnetic energy is fired, reflected, absorbed, suppressed, magnified, and used for a great number of military purposes.[5]

...the side who wins the next war will be the side with the last antenna standing. -- Norman Augustine, former Undersecretary of the U.S. Army and CEO of Martin Marietta Corp.

21st Century Environment

In many respects the 21st Century will look much like the 20th. The New World Order will not be so "new" or so "orderly". "The general level of instability in the Third World is increasing," because of the increasing dichotomy between rich and poor (15% of the population will control two-thirds of the wealth), just and unjust governments and quests for freedom and democracy.[6] "Overpopulation, rapid urbanization, environmental degradation and disease, rising nationalism and other phenomena will place severe strains on institutions, governments and alliances. Widely available and sophisticated conventional and nuclear armaments, coupled with new means to deliver them, will render the international arena even more volatile and unstable."[7] The most likely of these instabilities will be "low-cost, low-risk and high visibility " indirect aggressions, e.g. terrorism, insurgency, proxy warfare and drug trafficking.[8]

We have no crystal ball with which to plan for this future chaos, but ignorance of the future in detail is not a problem or weakness in planning, just a permanent condition.[9] Given such chronic uncertainty, we need a new framework that will help

strategically plan for future intelligence needs.

This new paradigm will be based on "uncertainty-pulled" instead of "threat driven" criteria, which died with the cold war. The U.S. will be pulled towards, "...generic kinds of challenges--intervention in regional conflict an ocean away,..." vice driven by detailed threats.[10]

We won't know whom, where, or when we'll fight again, but as noted above, multipolar relations and emerging nation-states may and probably will conflict.[11] The Marine Corps has published a watch list for their probable involvement as shown in Table 1.

WESTERN HEMISPHERE	MIDDLE EAST/ SOUTHWEST ASIA	AFRICA	ASIA/ PACIFIC	EUROPE/ MEDITERRANEAN
Argentina	Bahrain	Algeria	Afghanistan	Denmark
Bolivia	Egypt	Angola	Bangladesh	Greece
Brazil	Iran	Djibouti	Brunei	Italy
Colombia	Iraq	Ethiopia	Burma	Norway
Costa Rica	Israel	Kenya	Cambodia	Poland
Cuba	Jordan	Liberia	India	Turkey
Dominican Republic	Kuwait	Madagascar*	Indonesia	Yugoslavia
El Salvador	Lebanon	Morocco	Japan	
Grenada	Libya	Mozambique	Laos	
Guatemala	Oman	Namibia	Malaysia	
Haiti	Qatar	Somalia	N. Korea	
Honduras	Saudi Arabia	S. Africa	Pakistan	
Jamaica	Syria	Sudan	Papua N.G.	
Mexico	U. Arab E.	Tunisia	Philippines	
Nicaragua	Yemen	Uganda	PRC (Coast)	
Panama		Zaire	Hong Kong	
Peru		Zimbabwe	Taiwan	
Suriname			Singapore	
Venezuela			S. Korea	
			S. Pacific**	
			Spratly Is.***	
			Sri Lanka	
			Thailand	
			Vietnam	
19	15	17	22	07

* Includes Seychelles and Mauritius
** Includes Fiji, Kiribati, Vanuatu, New Caledonia, Solomon Is., and the general vicinity of Australia and New Zealand
*** Claimed by seven nations

Table 1: Expeditionary Environment Watchlist[12]

The consensus seems to be that future conflicts will occur on regional battlefields versus the Cold War planning for large-scale European conflict.[13] With that as a very general statement of the future world environment, let's briefly turn our attention to our national interests and priorities in 2020.

Interests, Priorities and Paradigms

With little hesitation, I will assert that our national interests over the next 30 years will look very much like those of today. Thus we will still be seeking:

1. The survival of the United States
2. A healthy and growing economy
3. A stable and secure world
4. Good relations with friends and allies[14]

From those continuing national interests military planners will derive the national military strategy and priorities. As Colin Gray has noted, while they will not know what the exact future demands will be, they can know the kinds of demands which will probably look much like today's, although the emphasis on particular aspects may be greater or lesser than today.[15] To protect the homeland, strategic nuclear and space forces, including ballistic missile defense, will continue to have first claim on our resources, even though the emphasis on the nuclear forces will continue to decline relative to today. Defense against whatever weapons of mass destruction exist will be foremost.

With the continuing trend of declining U.S. forces overseas and fewer overseas bases, the second priority will emphasize long-range maritime and air forces for long range power projection. Without them we will not be able to remain a world power and player to back up our other non-lethal means of national power.

Thirdly, we will still require some ground and tactical air forces, many unmanned, with which to conduct regional military operations.[16] . The principle players will probably be special forces for short notice contingencies to deter and, if necessary, fight small regional conflicts, terrorism, insurgencies and drug trafficking.[17] These forces will fight along side friends and allies whenever possible, but will need the capability to effect forced entry into an area if needed. These special forces will be backed up by more "conventional" forces, having much improved capabilities and mobility, but reduced manpower from the conventional forces of today. We must assume that such forces will face armies employing all of the technologies and weapons deployed today and most systems, if not all, that are in advanced development.

So while the national interests and priorities will show little, if any, change, the national military strategy and forces to support them will change considerably. They will drive demands for the future further explored below.

Those who minimize intelligence and think too much operationally may win opening set-piece battles, but the leaders who continually seek intelligence and then, with logistics constantly in mind, fashion their operations are the ones who win the tough campaigns and wars. -- BGen Hittle, USMC(Ret)

Future Force Drivers

Several factors will drive how the forces of the future will look in 2020. Current force composition, employment concepts/strategies, and technology will all play a part.

U.S. Force Composition. Since the military planning perspective extends 20 years out, our newest forces today and those currently on the drawingboard will make up the oldest forces in the inventory by 2020. Given a 10-20 year procurement cycle, the primary weapons will be those beginning development at the turn of the century.

With economic cuts probably continuing, this means that the military will have far fewer major weapons platforms, but they will have much greater complexity and cost. However, these systems will not be the classical tanks, manned aircraft or large capital ships, but smaller, more mobile, more costly and far more capable weapons. These vehicles will be complemented by a vast array of autonomous and nearly autonomous systems which will be even more mobile, smaller and less expensive, but still more sophisticated than today's weapons. Nearly all of these land, air and sea vehicles/platforms will require a combat identification system and active countermeasures to counteract electromagnetic guided munitions. Passive detection will

predominate.[18] Thus self defense will continue and probably increase in importance as assets become fewer in number and higher in value.

The U.S. force drawdown will reduce European and Pacific presence, and decrease forward-deployed, terrestrial support systems. "...[T]he next conflict may be a come-as-you-are war." where smaller, primarily U.S. based, expeditionary forces deploy not to reinforce, but to project global reach and power.[19]

The future air superiority fighter (F-22) now in initial flight test, will not be fielded until 2015 and will thus form the backbone of the air force in 2020. This aircraft is specified to have a first-look, first-kill capability. That will require a long-range, non-cooperative target identification system which must employ near-real-time tactical fusion of on-board sensors as well as correlation with incoming intelligence information. The F-22 will also have an on-board self-protection suite with a passive detection capability since it can expect to face highly developed air defense systems.[20] Both capabilities will require equipment providing excellent situation awareness -- multi-source, fused information for beyond visual range threat and target identification, confirmation and targeting.

Stealthy vehicles, be they air, land or sea, won't want to highlight themselves until absolutely necessary. This will call for fewer emissions while maintaining high situational awareness and warning. Aircraft are already beginning to employ missile approach warning systems (MAWS) that rely on hard to

detect, low probability of intercept signals. Follow-on systems to these embryonic efforts will complement "end-game" deceptions and off-board countermeasures. "End-game" generally refers to the last few seconds of a missile's flight before impact on a target. "Off-board" countermeasures are expendable countermeasures which are released/ejected from the defending vehicle and produce their desired effect in the vicinity of the target, generally in the last few seconds before impact.

Increasingly effective and lethal enemy defenses and higher value machines will continue to drive the development of stand-off attack weapons like the Joint Stand-Off Weapon now in development with an initial operational capability currently specified for 2003. This will often preclude aircraft from having to fly into the heart of the defensive threat envelope, greatly enhancing survivability. These precision guided, autonomous weapons will hasten the demise of the manned aircraft for missions against locatable ground targets, reconnaissance and battle damage assessment.

Moreover, non-lethal weapons, those which exist now and those in development, may be employed. But these non-lethal, disabling weapons have a price, and that price is increased reliance on timely, focused targeting intelligence -- better than that received in the Gulf War.[21] The down side to all of this is that there are,

> ...limitations to what can be done with realistic resource availability to completely satisfy the natural desire of military commanders to have up-to-date intelligence on all enemy activities...The United

> States will never be able to maintain a large enough group of ... signals intelligence processing personnel to deal with the flood of data produced by U.S. reconnaissance systems. Developments in computer processing of such data may help alleviate the problem, but even that is by no means a certainty.[22]

Employment concepts/strategies. To achieve the continuing desire to operate "... within the decision cycle of his adversary, tommorrow's commander must be able to observe the battlefield,..." which requires the identification of his opponents's order of battle, determining the status of his forces, and understanding the capabilities and weaknesses of his adversary(ies). While some of this information can be gathered in peacetime, the majority must be continually updated during the warfighting.[23] Or, as one author has put it,

> Because information is so central in modern warfare, every little technological or tactical issue that affects the speedy gathering, sharing and exploitation of information is of great importance.[24]

Thus the contest for information will dominate all aspects of warfare, with high tech war becoming a race to destroy the enemy's Command, Control, Communications, Computers and Intelligence (C4I) network before losing one's own to chaos, explosives and jamming.[25]

To win the contest, we must obtain and maintain control of air and space, which will be critical to preventing enemy reconnaissance and securing our own resources.[26] The U.S. or perhaps even a world body/international organization, "...will rely on space-based interceptors to negate threatening missiles,..." and will need a space based surveillance-and-

warning network to support it.[27]

The battlefield commander's key needs will focus on real-time intelligence to determine the threat on a more timely basis and rapid battle damage assessment (BDA). Achieving that will require a complementary mix of national level and tactical collection assets.[28] We must have combined sensors, those using diverse technologies or different portions of the frequency spectrum, to defeat jamming. Identification systems must allow for earlier, longer range identification of friend and foe. Direction finding will need to be improved at the tactical level for long-range weapons applications. On the ground these things will allow indirect fire weapons, long range artillery and rockets, to work more effectively when keyed by long-range sensors.[29] However, such weapons will require precise geolocacion data to cue their on-board sensors. Present "kilometer" accuracies will not suffice. Advanced precision guided munitions will need routine accuracies to a few meters, presently only available from imagery. Herein lies a significant challenge for operational SIGINT.

In the air, General Loh, the commander of Air Combat Command, has postulated a series of models to generally describe the environment and requirements when air forces are employed. This general paradigm will probably still hold for all air operations through 2020. In the aggregate the model calls for:

1. Probably fighting outnumbered and mainly deploying from the U.S. to reinforce an ally and any forces in theater.

2. Rapidly establishing a command, control, communications and intelligence (C3I) network in an immature theater.

3. Aircraft deploying within 24 hours of notification and perhaps defending themselves during theater entry.

4. Air forces would have to detect and destroy numerically superior enemy forces while avoiding surface-to-air threats.

5. They would operate autonomously or in conjunction with airborne and ground command and control (C2) elements.[30]

The keys to survival in all of this will be -- mobility, dispersion, stealth and defensive countermeasures. The inseparable duo of communications and intelligence will be the critical factors in achieving all of them.[31]

However, one of the greatest difficulties for the tactical commander will be "...separating the wheat from the chaff." What within the flood of information is really critical to him?[32] Moreover, operating in conjunction with allies will require policy decisions and guidance on how to provide raw, or half-assessed national intelligence to multinational coalition staffs. We will need quick, but adequate sanitization of sources.[33]

This high technology, information dependent warfare has already been conceptualized by the Chief of the Ground Forces of the old Soviet General Staff, Col Gen Grinkevich. His ideas on "Reconnaissance-Fire/Strike Complexes" exemplify the tight coordination required of intelligence, firepower and electronic

combat,

> The side that can count on victory is the side that first detects a target and attacks, is first able to make an aimed shot or volley, that is faster at completing its maneuver and overcoming obstacles, and that uses the results of weapons strikes without delay.[34]

Marshal Ogarkov, ex-Chief of the old Soviet General Staff has even gone further to suggest that,

> Rapid changes in the development of conventional means of destruction and the emergence in the developed countries of automated search and destroy complexes, long-range, high-accuracy terminally guided combat systems, unmanned flying machines, and qualitatively new electronic control systems make many types of weapons global and make it possible to sharply increase (by at least one order of magnitude) the destructive potential of conventional weapons, bringing them closer, so to speak, *to weapons of mass destruction* [nuclear and chemical weapons] in terms of effectiveness.[35]

This concept of warfare I expect to evolve over the next 20-30 years. It will involve far fewer numbers of weapons systems, but ones which are far more complex, costly and integrated. They will rely far more on each other and on an integrated, highly automated and "smart" C3I system to bring about this combat synergism and thus leverage. As the Soviets have prophesied, they may indeed replace armored divisions with much smaller units which, however, may function and cost as much as their predecessors.

Regardless of all else, however, ground or airborne operators will still want to know the very basics of:

Where is my target?

How do I get to it?

Did I kill it?

Technology Drivers. "During the 1990s, technological research and development will concentrate on multi-source data fusion;..."; the integration of databases, artificial intelligence and neural network technologies to solve the problem of information overload.[36]

One area which will receive a significant portion of this technological focus will be space systems that provide user friendly data streams. Microminiaturization and nanosecond computing will enable far more on-board signal processing, and therefore less reliance on terrestrial ground-processing and infrastructure. Such miniaturization and computation will also facilitate needed advancements, techniques and equipment, to fuse satellite data streams together at the collector source.[37]

Another technological effort, and probable recipient of data from the satellites mentioned above, will be the soldier's computer. This will be a pocket sized device with a helmet display which will include a radio function for communications and navigation as well as a combat identification capability to aide targeting and reduce fratricide.

From the mid-80s Tactical Digital Information Link (TADIL) suite of communications' protocols and standards, to today's Joint Tactical Information Distribution System, improved and integrated communications systems have been evolving.[38] The next generation is exemplified by the Navy's Copernicus Architecture which will "... acquire, standardize and concentrate

shore-based sensor and other data for Navy and joint uses. [It will be]...a 21st century force-multiplier effect stemming from the ability to concentrate sensors and data that is analogous to concentration of forces."[39] This kind of open communications architecture points to what VADM Macke of the Joint Staff has termed the "Infosphere". His concept visualizes a unified Pentagon data network which would handle most any type of data -- imagery, voice, data link, etc...that would be needed by U.S. forces deployed to crisis points.

"Standard-issue portable communications gear would allow a commander easy access to this data from anywhere in the world. 'When he goes out there, he kind of plugs in, like an electric light,'..."[40] He could turn on the intelligence data spigot and tap out only what he needs.

"Infosphere" would be a system of systems architecture allowing data and information to pass to any user, regardless of location or service. It would rely heavily on commercial, cellular-phone network technology and not be all satellite based, but also depend on long haul, wide bandwidth fiber optics.[41]

Motorola Corporation has already announced plans to launch 77 low-earth orbiting satellites to provide cellular voice and data capability by 1996 with their Iridium project. These "...will provide users with multimedia communication services on a mobile basis, employing handheld transceivers no larger than today's cellular telephones."[42]

As new technologies expand to new portions of the

electromagnetic spectrum, we may be able to use "...computer-based artificial intelligence systems to help analyze the mountains of data..."[43] The Advanced Planning System will take advantage of artificial intelligence, by using it to turn data (threat, terrain, order of battle, imagery, weather, etc.) into visual information, thereby reducing the 72 hour manual Air Tasking Order planning cycle by 75 percent, planning 2500 sorties every two hours.[44]

By the end of the century, laser weapons will be widespread throughout the world's armies.[45] Very powerful laser weapons will be capable of destroying enemy armored vehicles sometime in the future. They will eventually sweep unprotected infantry, sensors, and vehicles from the high-technology battlefield.[46]

Signal trends expected over the next couple of decades continue to point to the increased use of:

Millimeter waves (very high frequencies)
Very wide bandwidths
More complicated pulse patterns
Frequency modulations on each pulse
Pulse-to-pulse RF agility
Phased arrays using complex scans
Better sidelobe suppression
Radar internetting
Wartime reserved modes of operation
Very secure encryption devices/algorithms
A profusion of fiber optic and satellite communications

Mostly digital communications

These advanced, digitally based technologies will make signals more complex and harder to detect and identify than at present; artificial intelligence systems will be required to help overcome these advances.[47]

Already in 1992 the Services are planning aircraft warning systems which detect missile approaches using laser, millimeter-wave, infra-red and ultraviolet technologies. In the future we will have to fully integrate radar, IR, laser detection, warning and countermeasures into a coherent, multi-spectral warning and defensive system.[48]

Furthermore, we will have to seek ways to combine electronic combat and combat identification to overcome smart munitions and fratricide, especially in combat vehicles. The possibility of employing a laser bar code for identification purposes could well drive some ELINT/ESM needs. Nevertheless, on combat vehicles as well as aircraft, multi-sensor platforms with on-board data fusion capabilities for surveillance will be the order of the day.[49]

Thus technology will in part drive the future high technology battlefield. The growth of computer workstations and sophisticated sensors will have made global surveillance a real possibility.[50] But as VADM Tuttle, Director of the Navy's Space and Electronic Warfare Directorate, has noted, one of the biggest challenges we face as we move into the 21st century, will be to develop new technologies to integrate sensors and solve

communications capacity problems.[51]

As we have seen, our current and planned force composition, future warfare demands and technology pushes will have a profound impact upon the kind intelligence system that we will require in the future. Let us now more directly turn our attention on how those futuristic factors will shape and impact on that system.

What in your long military service was your biggest problem? ... trying to determine what was on the other side of the hill. -- Duke of Wellington

Impact on Intelligence

Before we examine how future warfighting concepts and technologies will impact upon intelligence, let us digress to look at intelligence lessons learned from the last war.

Gulf War Lessons Learned. "The Gulf War was fought with more intelligence information and materials available to the tactical commanders than any other war in U.S. history. The problem was that it was not always in the right hands at the right time and place." General Schwarzkopf stated that we "...just didn't have a responsive intelligence capability that will give the theater commander near real time information as he personally needs to make a decision."[52]

The primary criticism centered around processing and dissemination, that there must be far better intelligence system interoperability to more quickly collate and disseminate information to commanders, particularly at echelons below

corps/numbered air force. There were too many people handling, reformatting and passing info, slowing things down.[53]

Part of the solution is a priority emphasis placed on "...secure intra-theater data communications capable of supporting simultaneous transmission of order of battle, threat and target data to all nodes and units."[54]

The initial successes of providing tailored, broadcast intelligence information services were undertaken with the Constant Source[1] and the Theater Intelligence Broadcast System (TIBS). These two systems provided near-real-time, multi-source signals intelligence by receiving and decoding satellite and RC-135 aircraft broadcasts of intelligence information. Such data helped aircrews locate Iraqi anti-aircraft batteries and fighter bases within 10 minutes of detection by signals intelligence collectors.[55] Another system, which used Air Force missile warning satellites, broadcast reports on Iraqi missile launches and relayed that information to Patriot missile batteries.[56] Thus, as one author has put it, "...intelligence broadcast[s] to users through C4I [Command, Control, Communications, Computers and Intelligence] must be now regarded as a battlefield force multiplier; ... that must, in the final analysis, be concentrated on the battlefield to win the battle."[57]

Following up on this experience the Air Force "... is

---

[1] The Air Force's Constant Source, Army's Success Radio and the Navy's TRAP/TRE all refer to the same broadcast system based on the Navy's earlier development work. Constant Source will be used in this paper to refer to any one of these equipments.

planning to procure 300 Constant Source terminals by 1998, half of them airborne equipment due to become available in 1993."[58]

Meanwhile the Army will upgrade its airborne, tactical SIGINT collector (Guardrail) and its current Commander's Tactical Terminal (CTT), which displays intelligence information to the ground commander. The upgraded version of the Improved Guardrail V, called Guardrail/Common sensor, will integrate COMINT & ELINT collection and processing.[59] The CTT-Hybrid upgrade program will merge Constant Source data into CTT displays along with the Guardrail and other data.[60]

As a result of the war the Air Force is creating an improved intelligence system to provide widespread and more timely dissemination of intelligence data via on-board collector processing and near-real-time broadcast systems from collector and all source organizations.[61] A part of that system will be a Tactical Air Force Linked Operations/Intelligence Center to provide a baseline, "...graphic display of the ground situation through correlation and aggregation of all-source intelligence."[62] It will be designed to be interoperable with the Army's similarly functioning All Source Analysis System (ASAS).

As the Department of Defense's final report on the Gulf War acknowledged, "...[C]ompletely eliminating all the [intelligence] short-comings is not possible within existing budgetary and personnel limitations." However, the report goes on to say that the "'...detail desired in some cases was, and will continue to

be, beyond the capabilities of the intelligence system.'"[63]

These above observations and challenges we will take into the 21st Century. As we reorient our strategy from a post-WWII, Cold War containment outlook, to one based on regionally oriented, expeditionary forces, one general on the Joint Staff has articulated several key issues that must be addressed--

1. Readiness
2. Collective security
3. Arms control
4. Power projection
5. Technical/technological superiority

These will form a framework on which I will attempt to hang some intelligence challenges for the future.

Readiness. For the intelligence community, readiness will imply very short tactical warning time while satisfying increased demand for more intelligence information on non-Soviet targets.[64]

While we believe that strategic warning for major conflict will be substantially longer, regional conflict and subsequent U.S. deployment will continue to occur on a reduced time scale. Indeed, as Gen Loh envisioned, aircraft would be airborne in 24 hours. This will require that peacetime databases which support operational forces, must be continuously kept updated on far more diverse targets and geographic areas than under the Soviet monolith. It also implies that the intelligence system must orient itself so that it can provide real time updates (SIGINT and IMINT) to forces enroute, while they are still airborne.

The efforts with Constant Source and TIBS to date, and their successor, the Multi-Function Advanced Tactical Terminal, are steps in the right direction, but must be refined and evolved to a much higher degree of information sophistication (spelled integration, correlation and fusion) while becoming far more user friendly in the future. Most users, especially the "shooters", will not care what source gave them the information or the tremendous technical and political challenges needed to get it to them. They just want up to date information when they request it.

One senior NSA official has articulated this problem as shown in Figure 1. The figure shows the relationships between

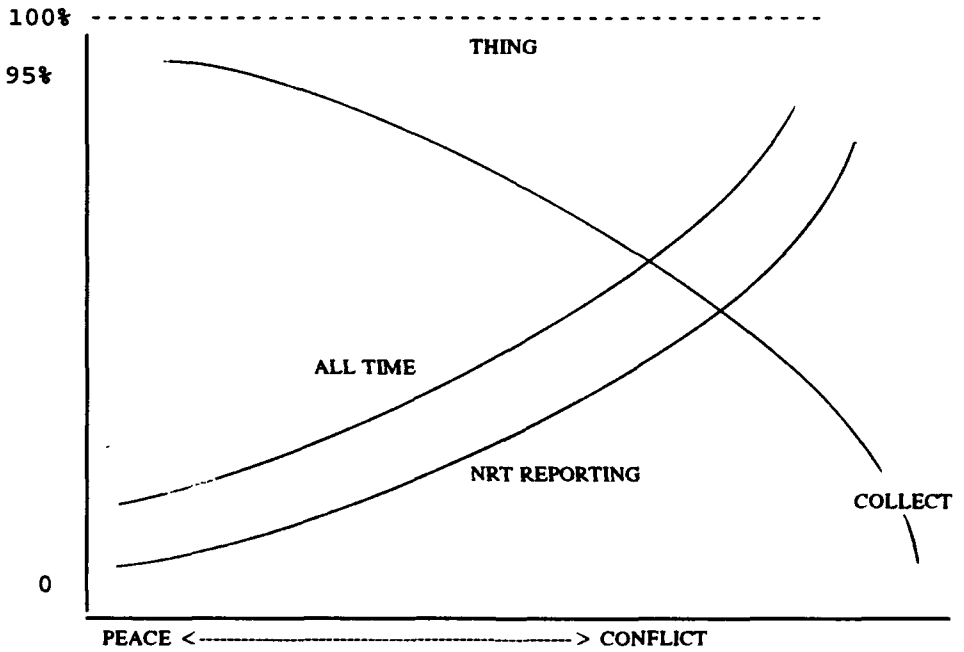


Figure 1. Collection and Reporting Continuum

the continuum from peace to conflict on the bottom axis with the

percentage of reported information along the vertical axis. The figure was built on ELINT data, but could be extrapolated in a general sense to all source reporting. As the figure depicts, in peacetime the goal should be to pluck everything out of the ether, but report only a small percentage in either near-real-time or all the time. The difference being that the user will want a small number of signals reported regardless of how often they occur or don't appear to change. The vast majority of the data will be stored up in on-line data bases so that operational and technical analysis can be performed on it as required.

As one transitions to a conflict, the amount of information to be reported out increases, but the overall collection take focuses down to a smaller area of interest and hence, less overall collection. Thus we must tailor and refine intelligence broadcasts so that they can usefully and graphically be displayed in near-real-time and reduce the significant amount of ambiguous and useless data that we are now transmitting over such broadcasts through advanced signal correlation techniques. Nevertheless, until artificial intelligence can catch up to its hype for real performance, we must have trained operators at the receive terminals of our intelligence broadcast systems to ferret out bogus signals, collector vagaries and apply professional intelligence and tactical operations judgement. A combination of electronic warfare and intelligence disciplines is required. More information transmitted more quickly implies more room for errors and ambiguities. It is especially important for Constant

Source and TIBS to have these smart operators select out duplicate reports and remove emitter data which is no longer valid or desired. Even with true data fusion and other technological marvels, all of these advanced intelligence systems serve only, "...to assist intelligence specialists, not to replace them."[65]

Readiness also requires that intelligence analysts undertake a more "opportunity-oriented analysis" approach. Such analysis complements purely descriptive analysis by focusing on vulnerabilities suggested by the information. One author claims that this more complex and risky form of analysis has been undertaken only rarely and generally reluctantly, but with a few exceptions such as, "...analytical products that anticipate defensive countermeasures an enemy might use." These analyses have been produced and do highlight and key on vulnerabilities, but are rare gems indeed.[66] Quick reaction, especially Special Operations Forces, will live or die by these vulnerabilities assessments and airborne updates, especially during forced entry scenarios.

Collective Security. As stated in the United States strategy, we seek to share global leadership and global responsibilities. Thus we expect to fight along-side allies who will demand and need critical intelligence that only the United States can provide. As noted earlier, one of the critical questions will be how to sanitize and share intelligence with new/non-traditional allies while protecting sources. We must

plan for that eventuality, not hide our heads in the sand and hope that we can *ad hoc* the situation at the time.

A part of that sanitization problem has not only to do with allies, but also our own forces, since even U.S. operators bemoan the fact that the higher the classification, the less useful it is to them. A corollary also states that the longer an intelligence report is, the less likely it is to be read.[67] Succinct, sanitized, but all source, non-paper reports will be the order of the day. Indeed, provision of such intelligence support may be one of our principal contributions to future coalitions while keeping our manpower commitments low.[68]

Arms Control. As Anne Armstrong, Chairman of the National Foreign Intelligence Board, has noted, the START and INF treaties, "...will require new investments in technical intelligence collection capabilities."[69] While the primary impact has been upon imagery intelligence, signals intelligence will play an increasingly important role, not only using FISINT, but other COMINT and ELINT inputs can be expected to have significant impact. But even in this area, the key will remain the correlation and fusion of intelligence.

Power Projection. When U.S. forces are deployed and employed into regional crises, the reconnaissance/strike concept will require user friendly, fused, near-real-time intelligence support which is focused on critical targets. While ELINT will continue to be a vital tactical input, what is really needed is data fusion. We can presently collate and consolidate data well,

but,

> ...there is no known technique of taking multiple inputs and 'doing something with them in a black box, and they come out and tell you all you want to know about the target, and that's what fusion is.' True data fusion will require a technological breakthrough in order to give commanders and operators the composite, graphical view of their piece of the battlefield that they will require.[70]

In this quest air intelligence is the toughest challenge since, "[u]nder a centralized intelligence structure spread out over hundreds of miles, dissemination becomes absolutely critical."[71]

As intelligence becomes more responsive to operational users, operations and intelligence functions and their interface become ever more dependent on electronic pathways.[72] The communications system needed to disseminate this data will be just as important as the collection, processing and analysis of the data itself. A dedicated, secure C4I system, probably based on a forward deployed SATCOM link, will be needed to carry a high volume of ops immediate, all source material. The system must have enough capacity to simultaneously handle secure voice, fax/imagery, teleprinter and data link. Above all else, however, it must be a reliable, secure broadcast system for user nodes at all levels, tactical to national, since data access will be required from mobile ground stations, ships or aircraft.

Technical/Technological Superiority. I have postulated that future forces will employ fewer, higher value systems. For conventional weapons, this will imply more modifications and evolutions, furthering the already present trend of adding

adjunct sensors or targeting systems to complement a weapon that already exists. Such "...qualitative changes are much more difficult to assess than quantitative ones" and will thus make the intelligence analyst's job that much more difficult, especially when such equipment will be a blend of foreign and friendly manufacture.[73]

As vehicles begin to routinely employ missile approach warning systems (MAWS), "end-game" and "off-board" countermeasures, what does this portend for classical technical SIGINT? And more specifically ELINT? MAWS will reduce the reliance on ELINT and even fused SIGINT to provide immediate missile launch warning. Until such time that high powered microwave or laser weapons technologies are employable on combat vehicles to destroy these incoming weapons, the only defenses to counter these threats will rely on technical intelligence collection and analysis. How much SIGINT will provide is debatable, since "end game" information is very difficult to collect. Perhaps HUMINT and the exploitation of foreign and friendly systems will play the bigger part.

Another major factor contributing to a stealthy vehicle's success is its avoiding threats as much as possible. Stealth does not make a vehicle invisible to radar, but reduces that signature in various ways. Thus the pattern that a threat radar has as a function of its design is of great interest to stealthy vehicle mission planners in order to reduce the vulnerability of their limited number of very high value assets. Here, only ELINT

can deliver the needed technical data.

As sensors and weapons systems evolve to more exotic technologies, laser, ultraviolet, high power microwaves, etc., less information on these technologies is known in general so that there are fewer analogues with which to compare and reference intelligence estimates. Since these technologies are generally less observable, hence one of the reasons for their evolution, there will be greater difficulty in collecting and understanding what is collected.[74]

Greater technological complexity will force analysts to be much more explicit in expressing "...what they know, what they do not, and how they came to know what they think they know." in technical assessments. They will not just be able to gather facts and infer trends, but must make more explicit their analytical bases and paradigms, ensuring that users are aware, "... what premises underlie major analytical products."[75]

> *Whether it's keeping track on international narcotics trafficking, weapons proliferation in Third World countries, or supporting a war in an unexpected place, the demands placed upon intelligence have never been greater.* Sen Boren -- ex-Chairman of the Senate Select Committee on Intelligence[76]

Intelligence Futures

If the United States is going to be a global actor in the new world order, it will need a global intelligence system. We now stand at a crossroads driven by fiscal austerity and

political "hostility" toward intelligence organizations. Without prudent leadership and analytical thought about what intelligence will really be needed in the decades ahead, we could cut programs that would take decades to rebuild. Perhaps the greatest key factor is ***the need to plan for global flexibility in intelligence. Such flexible capacity, will not be based on a threat.***[77] Instead, again invoking Collin Grey's idea, we won't know what specific threats there will be, but only that there will be certain kinds of threats.

In this new world order, some foresee a "911" syndrome, where the U.S. response is the only viable one. This will be the hardest intelligence mission of all, since as our forces shrink, ever more capable intelligence support to operations will be required. This calls for extreme caution in cutting intelligence institutions, manpower and programs.

In the future, strategic intelligence will largely focus on "intentions" of adversaries real and potential. The priorities over at least the next decade will center on the following issues which are not listed in any particular priority order:

1. Proliferation of weapons of mass destruction and their delivery systems
2. Counter terrorism
3. Counter narcotics
4. Counter intelligence
5. Economic and trade issues

6. Technology developments which could damage U.S. interests.

7. Russia and FSU nuclear states

8. Key countries -- Germany, Japan, France, etc.[78]

Our future collection systems must be designed with growth potential -- the ability to rapidly tailor themselves through technology insertion and reprogramming. They must cover not only known frequency ranges, but also commercial emitters that might be employed off the shelf.[79] It must be a system of systems since no one system can cover all threats. Some of these like the Army's Guardrail system, will be directly tasked by the local commander. Others will belong to or be tasked by higher echelons up through the national level. The key requirement is that all must be based on a common architecture and components so that they are able to inter-operate in real time.[80]

Not all of the answers to future intelligence challenges will be found in the flexible capacity of our systems or their infusion of technological improvements. Some cultural changes in the way we organize and view intelligence organizations will also have to evolve. As noted in the FY 91 Intelligence Authorization Bill,

> ...The tactical and national Intelligence Communities appear to be excessively isolated from one another, leaving each free to pursue self-sufficiency in their particular realms. Military commanders seek self-sufficiency through organic systems and organizations on the argument that national systems or civilian systems cannot be relied upon for support. The national community, likewise, emphasizes its peacetime missions and pays scant attention to the commander's needs.[81]

While I feel that there is too much isolation from one another, despite improvements during and after Desert Storm, I would also assert that we will need both a "strategic" or "national" intelligence component as well "tactical" or "operational" support.

The local commander must have some organic assets which he can task and control for his immediate intelligence needs. Likewise our national command authorities, the President, National Security Council, Secretary of Defense and Joint Chiefs, need "national" level organizations to filter through the myriads of military, political, economic and social information which have strategic impact on all types of national policies and which respond to their needs. We must overcome the cultural bias that "control" of an asset does not limit information access to intelligence derived from that asset. Thus the local commander's intelligence systems, while tasked and controlled by him for his purposes, need to funnel resulting intelligence upward all the way to national level databases and analysts, without being driven/tasked by them. The emphasis must be on support to the local commander, but reporting to the larger system. On the other hand, national, "strategic" assets would emphasize satisfying needs of national decision makers, but report/broadcast information to the local commander which complements his organic assets. This would especially be true of near-real-time broadcasts as described earlier. There must continue to be a blending of these complementary assets and

missions. They must be interoperable with common formats and communications architectures, but must also be culled of competing functions and capabilities where it no longer makes sense to fund such duplication. As noted in post-WWII and DIA reports, there are strengths in both -- both are needed. The amount or level of each and their reporting and tasking are the real issues.

Conclusion

Most, if not all of the areas discussed above, are not new and there are many programs already underway to tackle most of these problems. The momentum initiated by these programs must be continued. But intelligence processing and dissemination systems and their accompanying programs are not "sexy". A Congressman can't point to a fiber optic cable or a computer switching network and gain home town votes on the nightly news. They don't have the verve like a new, classified DOD payload a.k.a. intelligence "spy" satellite or an alleged SR-71 follow-on reconnaissance aircraft called Aurora. They are most similar to water and sewer projects which build infrastructure. But let them get neglected and unfunded, and wait for the howl from commanders who decry that they can't get the intelligence they need and don't understand why they can't have it.

But assuming that at least some of these programs survive, ***the key is to not let them become new collection programs, but maintain their emphasis on the processing and dissemination which will provide the force multiplier.***

We can't afford a plethora of tactical intelligence systems in the field. Tactical forces can't afford the cost, volume or weight of numerous, non-interoperable intelligence tools and systems. We need a common set of displays, user tailorable, hosted on a processor with multiple feeds and ideally using a common format/bit stream. Format and interface standards are a must. Hopefully the fourth generation follow-on to Constant Source/TIBS, which is in the design stages, will solve the problem of having a single system to fuse all source information into a single integrated display and processor.

The intelligence community needs to practice data dissemination and fusion with operations folks on daily basis. Intelligence personnel can't wait until crises to "turn on the intelligence spigot from behind the green door" and expect operators to know what they want, how to use it and trust the information they're getting, without building up a body of experience and trust in their intelligence systems and personnel. This means providing real world collection and information on a regular basis.

Furthermore, all intelligence organizations need to exercise and surge their collection, analysis and dissemination capabilities just like military units surge and exercise to operate their systems and people under stress. Even with intelligence reorganizations to aline peacetime/wartime functions, no stress on the systems/organizations makes for re-learning previous "lessons learned".

To keep the emphasis on interoperability, national agencies should research and develop national systems and define the intelligence architectural standards for their intelligence collection discipline -- HUMINT, IMINT, SIGINT. The Director of Central Intelligence should define and enforce community-wide standards which will ensure the interoperability within and across each collection discipline as well as across all data dissemination systems.

Another rule which the intelligence community must learn to apply to their product is the 80 per cent rule. Just like in the acquisition community, the last 20 per cent of performance improvement will take an inordinate amount of time and dollar investment. For intelligence, time is the greatest enemy. Perfect intelligence next week is useless to a commander who needs an answer, a best judgement, today. The intelligence community must focus on providing an 80 per cent solution, with some judgmental risk, and train our leaders that that is the situation.

As budget cuts continue, intelligence professionals must well articulate the need for technical intelligence, as well as operational intelligence in support to military operations. Technical intelligence is the whole life policy -- we pay a premium/cost over the long term in peacetime to guard against sudden death, technological surprise. We must pay the price if we are going to avoid technological surprise and continue to field and use countermeasures for fewer, higher value systems.

One must not forget that much of the technical victory in Desert Storm was built upon 20 years of technical intelligence analysis of Soviet, Chinese and western manufactured weapons systems.

To continue to leverage ourselves by employing technology in lieu of U.S. lives in battle, the U.S. must stay technologically ahead both militarily and commercially. Militarily this means that we must have early alerts of new and/or modified systems. New tip offs and alerting keys are required since old paradigms are not translatable to the future. Commercially, we must stay one step ahead of the friendly competition (Western Europe, New Zealand, Australia, Canada, Japan, Russia, and Israel) for economic well being/competitiveness and two steps ahead of the rest of the world.

There are systems out there now which look the same on imagery, but emit greatly different signals. There are systems for which technical data, exploitation and HUMINT sources say operates in some fashion X, but it really operates in different modes X,Y, and Z. Sometimes these modes are even unknown to the design engineers of the system! Technical SIGINT can provide those answers, sometimes to questions that haven't even been formulated, but are critical.

HUMINT, foreign materiel exploitation, and IMINT may give a base line, but SIGINT can determine some modifications to systems. It can key HUMINT and IMINT to re-look and further collect info on a system which has been modified from a previous baseline. In many cases only technical SIGINT will provide the

ground truth for threat receiver and countermeasures development. As one expert has put it, "If it radiates, we need to confirm it." It will tell you what the signal really looks like, not what someone/something says it looks like. But it can't do everything since there is little to no information derived from SIGINT on the receivers and data processors of systems. Thus, in technical intelligence, like its operational complement, fusion of all data sources is needed.

The future belongs to focused, fused, friendly intelligence -- the "cheaper" force multiplier of the 21st Century. The challenge will be to keep the systems and organizations focused on interoperability while providing technical and operational support to the warfighter as well as satisfying national consumers.

1. "Vetronics is the term given to the integration of all vehicle electronic systems -- digital, audio, video, electrical power distribution and computer resources." Bustin, p. 82.

2. Tapscott, 46.

3. Munro, 158.

4. Schleher, 8.

5. Munro, 2.

6. Locher, 11.

7. Locher, 11.

8. Ibid.

9. Gray, 19.

10. Gray, 18-19.

11. Moorman, 17.

12. Steele, 74.

13. Loh, 6.

14. The White House, 3.

15. Gray, 22.

16. Gray, 21.

17. Locher, 12.

18. Ackerman, 35.

19. Loh, 6 and Moorman, 18,19.

20. Loh, 12.

21. Ricks, 1.

22. Richelson, 37.

23. Hamel, 11.

24. Munro, ix.

25. Munro, 275, 257.

26. Munro, 305.

27. Moorman, 21.

28. Gagner, 41 and "Combat Commanders' Needs Color Intelligence Planning" ,45.

29. Munro, 307.

30. Loh, 9,10.

31. Munro, 305.

32. Hughes-Wilson, 43 and Tapscott, 25.

33. Hughes-Wilson, 42.

34. Munro, 189.

35. Munro, 189-90.

36. Lok, 1031.

37. Moorman, 21.

38. Griffin, 52.

39. Loescher, 89.

40. Grier, 113.

41. Grier, 115.

42. Banford, 90.

43. Godson, 54.

44. Struck, 28.

45. Ricks, 1.

46. Munro, 40 and Richardson.

47. Richardson.

48. Richardson, 408.

49. Struck, 33.

50. Loescher, 86.

51. Loescher, 86.

52. Leonhardt, 21.

53. Starr, 636.

54. Clapper, 79.

55. Buenneke, 23; Clapper,77; Richelson, 36.

56. Buenneke, 23.

57. Hughes-Wilson, 43.

58. Chenard, 4.

59. Struck, 31.

60. Richelson, 36.

61. Clapper, 79.

62. Clapper, 80.

63. Richelson, 37.

64. Godson, 52.

65. Jenkins, 17.

66. Godson, 49.

67. Steele, 73.

68. Seaquist, 48.

69. Armstrong, 25.

70. Williams, 69.

71. Ingram, 65.

72. Banford, 91.

73. Godson, 53.

74. Godson, 53.

75. Godson, 50.

76. Hearing Before the Select Committee on Intelligence of the United States Senate, 2.

77. The White House, 19.

78. "Intelligence Reorganization Springs From Inside Forces", 28; and Williams, 33.

79. Campbell, 45.

80. Campbell, 46.

81. Hearing Before the Select Committee on Intelligence of the United States Senate, One Hundred second Congress, 1st session on review of Intelligence Organization, 3.

REFERENCES

Ackerman, Robert K., "Electronic Warfare Explodes As Threats Spawn Diversity", Signal, Mar 92, Vol 46, No.7.

"Aircraft Sensors Unmask Foes, Anytime, Anywhere," Signal, Sep 92, Vol 47, No. 1.

Armstrong, Anne, "Bridging the Gap: Intelligence and Policy", The Washington Quarterly, Winter 1989, Vol 12, No.1.

Ball, Desmond, "The lethal, critical and costly intelligence war", Asia-Pacific Defence Reporter, Feb 91, Vol 17, No.8.

Banford, Harry C., Meteoric Changes Forecast In Intelligence Processes", Signal, July 1991, Vol 45, No. 11.

Brown, James O. Jr., "Electronic Countermeasures Clobber Air Defense Radars", Signal, Mar 92, Vol 46, No.7.

Buenneke, Richard H. Jr., "Lifting the Fog of War", Government Executive, Feb 91, Vol. 23, No.2.

Bustin, Ian, "Vetronics -- The Quiet Revolution For Armoured Vehicles", Military Technology, 5/92, Vol XVI, No.5.

Campbell, BG William H. and Hayden, William, "Intelligence is for Commanders", Journal of Electronic Defense, Oct 1992, Vol 15, No. 10.

Chenard, Stephane, "Lessons of The First Space War", Interavia Space Markets, Jul 1, 1991, V.07, No. 04.

Clapper, MGen James R. Jr., "Desert War Was Crucible For Intelligence Systems", Signal, Sept 91, Vol 46, No. 1.

"Combat Commanders' Needs Color Intelligence Planning", SIGNAL, Aug 92, Vol 46, No.12.

"ELINT Challenges", a briefing given to senior NSA management prepared by NSA staff, 1992.

Gagner, Wayne P., "Surveillance Proves Primary Need in Tactical Collection", SIGNAL, August 1992, Vol 46, No.12.

Godson, Roy, "Intelligence Requirements for the 1990s", The Washington Quarterly, Winter 1989, Vol. 12, No.1.

Gray, Dr.Colin S., "Defense Planning For The Mystery Tour", Air

Power Journal, Summer 1991, Vol V, No. 2.

Grier, Peter, "Prognosis Less Bleary Than in Other Sectors", Government Executive, Aug 92, Vol. 24, No.8.

Griffin, Louisa, "Tactical Data Links Promote Tri-Service Interoperability", Defense Electronics, June 92, Vol. 24, No. 6.

Hamel, LtCol Michael A. and Wolfert, LtCol Michael L.,"Space Strategy and the New World Order", AFSPACECOM/XPX, April 1992.

Hearing Before the Select Committee on Intelligence of the United States Senate, One Hundred Second Congress, 1st Session on Review of Intelligence Organization, Thursday, March 21, 1991. Docs Y4.In8/19:S.HRG.102-91/c.1

Hittle, BGen James D., "Intelligence Reorganizers Should Be Careful", Marine Corps Gazette, July 92, Vol 76,No.7.

Hughes-Wilson, Col John, "Battlefield Intelligence For The Future", NATO's Sixteen Nations, Dec 91, Vol 36, No.7.

Ingram, Col David H., "Fixing Intelligence: It's Decision Time, Marine Corps Gazette, Jun 92, Vol 76, No.6.

Institute for National Strategic Studies, "Project 2025", National Defense University, 6 May 1992, Working Paper, Limited DoD distribution.

"Intelligence Reorganization Springs From Inside Forces", SIGNAL, August 1992, Vol 46, No.12.

"Intelligence Support to Policy", briefings given to the ICAF Class of 1993, National Defense University,

Jenkins, MajGen Harry W. Jr., "Tactical Intelligence and Related Activities: Report From the Director of Intelligence", Marine Corps Gazette, Sep 92, Vol. 76, No.9.

Leonhardt, Maj Kent A., "All the Intelligence in the World Is Useless Without the Means To Disseminate It", Marine Corps gazette, Mar 92, Vol 76, No.3.

Locher, James R. III, "Focusing on the Future: The role of SOF in emerging defense strategy", Special Warfare, Mar 92, Vol 5, No.1.

Loescher, Lt Commander Michael S., "Copernicus Offers a New Center of the Universe", Naval Institute Proceedings, Jan 91, Vol. 117/1.

Loh, Gen John M., "Advocating Mission Needs In Tomorrow's World", Airpower, Spring 92, Vol VI, No.1.

Lok, Joris Janssen, "The future for C3I", Jane's Defense Weekly, 24 Nov 90, Vol 14, No.21.

Moorman, LtGen Thomas S. Jr., "Space A New Strategic Frontier", Airpower, Spring 92, Vol. VI, No.1.

Munro, Neil, The Quick and the Dead, St. Martin's Press, New York, 1991.

"Optical Tape Recorder Can Store Terabyte of Data", Defense Electronics, Jun 92, Vol 24., No.6.

Richardson, Doug, "Trends in self-protection EW systems", INTERNATIONAL AEROSPACE REVIEW, May 01, 1990, Vol. 45, No. 05.

Richelson, Jeffrey T., "Volume of Data Cripples Tactical Intelligence System", Armed Forces Journal International, Jun 92.

Ricks, Thomas E., "Nonlethal Arms", Wall Street Journal, Jan 4, 1993.

Schleher, D. Curtis, Introduction to Electronic Warfare, Artech House, Norwood, MA, 1986.

Seaquist, Larry, "Defense Intelligence in a Disorderly World", Defense Intelligence Journal, Spg 92, Vol 1, No. 1.

Soyster, LtGen Harry E., "System Extends Real-Time Intelligence to Theater Level", Signal, Sept 91, Vol 46, No. 1.

Starr, Barbara, "Measuring the success of the intelligence war, Jane's Defence Weekly, 20 April 1991, Vol 15, No. 16.

Steele, Robert D., "Intelligence Support for Expeditionary Planners", Marine Corps Gazette, Sep 1991, Vol 75, No. 9.

Struck, Myron, "CECOM's EW/RSTA: Developing A New Generation Of Electronic Warfare Systems", Defense Electronics, Oct 91, Vol 23, No.10.

Struck, Myron, "Rome Laboratory -- Creating Basic Technologies for C4I", Defense Electronics, Sep 91.

Tapscott, Mark, "CECOM: Ensuring A Battlefield Edge Through Advanced Technologies", Defense Electronics, June 92, Vol 24, No.6.

Tapscott, Mark and Struck, Myron, "U.S. Intelligence Agencies At An Historic Crossroads", Defense Electronics, Nov 1991, Vol 23, No.11.

Terry, Maj Neri G., "It's Time to Integrate Jamming Into Our Ground Operations, Marine Corps Gazette, March 1992, Vol 76, No.3.

The White House, The United States National Security Strategy, 1991.

Vollrath, Col Thomas L., "ELINT ESM for the IEW Common Sensor System", Journal of Electronic Defense, Oct 92, Vol 15, No. 10.

Williams, Robert H., "U.S. Intelligence Responds To Changing '90s Missions", Signal, Sep 91, Vol 46, No.1.

Williams, Robert H., "Congress Reserves Option to Reorganize Intelligence", SIGNAL, August 1992, Vol 46, No.2.

COLONEL LEWIS S. HENDERSON, III

Colonel Lewis S. Henderson, III is a student at the Industrial College of the Armed Forces, Fort Leslie J. McNair, Washington, D.C.

Colonel Henderson was born on 12 Nov 50, in Pensacola, Florida, and graduated from Parsons High School, Parsons, Kansas, in 1968. He earned a Bachelor of Science Degree in Aeronautical Engineering from the United States Air Force Academy in 1972, and a Master of Science Degree in engineering from the University of Texas, Austin, Texas, in 1983. He completed Squadron Officer School in 1974, Air Command and Staff College in 1981, and the Air War College in 1987.

After receiving his commission, Colonel Henderson served as a Deputy Missile Combat Crew Commander, Deputy Flight Commander, and Wing Standardization/Evaluation Examiner in the 351st Strategic Missile Wing, Whiteman Air Force Base, Missouri. After navigator and electronic warfare officer training at Mather Air Force Base, California, 1974-76, he was assigned as a Remotely Piloted Vehicle Launch Control Officer with the 349th Strategic Reconnaissance Wing, Davis Monthan Air Force Base, Arizona. He subsequently served as an RPV Remote Control Officer, Senior Instructor, and Drone Mission Commander in the 43d Tactical Drone Group.

From June 1979 to July 1981, Colonel Henderson was attached to the Air Force Flight Test Center, Detachment 3, as the Officer in Charge of Flight Test Operations for a presidentially-directed Joint Test Force special access program. Selected to attend graduate school under the senior commanders' education program, he graduated in 1983, and became a Branch Chief in the Electronic Warfare Staff at the National Security Agency (NSA), Fort Meade, Maryland. He subsequently became the Deputy Chief of the Electronic Warfare Technology and Support Staff.

In 1987 he moved to the 65th Air Division, Lindsey AS, Germany where he served as Chief, Combat Intelligence and Requirements, and as Assistant Director and Director of Operations. Colonel Henderson took command of the 7580th Operations Squadron, Rhein-Main Air Base, Germany, in June 1989. He moved up to become the Deputy Commander for Operations, 66th Electronic Combat Wing, Sembach Air Base, Germany in September 1990.

Returning from overseas, he returned to NSA in 1991 as the Deputy Chief of the Defensive and Ground Weapons Systems Division, Office of Weapons and Space Technology. He assumed his present duties in August 1992.

Colonel Henderson is a master navigator/electronic warfare officer with over 1,000 flying hours. His decorations include the Joint Meritorious Service Medal, Air Force Meritorious Service Medal with two oak leaf clusters, Aerial Achievement Medal, Air Force Commendation Medal with two oak leaf clusters, and the Combat Readiness Medal.

Colonel Henderson is married to the former Cheryl A. Williams of Sacramento, California. They have three children, Brianna, Bradley, and Benjamin.